

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Previously Presented) A digital identity device, comprising:
 - a microprocessor comprising a microprocessor identity that uniquely identifies the microprocessor, wherein the microprocessor identity is stored in the microprocessor;
 - digital identity data, wherein the digital identity data uniquely identifies a user of the digital identity device;
 - a memory configured to store at least the digital identity data, wherein the digital identity data is bound to the microprocessor identity by encrypting the digital identity data using an algorithm that uses the microprocessor identity.
2. – 5. (Cancelled)
6. (Previously Presented) The digital identity device of claim 1, wherein the digital identity data comprises at least one selected from the group consisting of a name, a digital picture, an address, a date of birth, a social security number, a driver's license number, a digital photograph, biometric information, credit card information, bank account information, an incorporation name, a date and place of incorporation, a name of a corporate officer, a corporate partner, and a database administrator name.
7. (Cancelled)
8. (Previously Presented) The digital identity device of claim 1, wherein the digital identity device further comprises an interface configured to enable the digital identity device to communicate with an external device.
9. (Previously Presented) The digital identity device of claim 8, wherein the interface comprises an input/output port.
10. – 29. (Cancelled)

30. (Currently Amended) A method of identifying an origin of an electronic communication, comprising:

tagging the electronic communication to obtain a tagged communication, wherein the origin comprises a digital identity device comprising digital identity data that uniquely identifies the origin; and

determining the origin of the electronic communication using the tagged communication, wherein tagging the electronic communication comprises:

encrypting the electronic communication using the digital identity data and an encryption algorithm to obtain the tagged communication, wherein the digital identity device comprises:

a microprocessor comprising a microprocessor identity that uniquely identifies the microprocessor, wherein the microprocessor identity is stored in the microprocessor, and

a memory configured to store at least the digital identity data, wherein the digital identity data is bound to the microprocessor identity by encrypting the digital identity data using an algorithm that uses the microprocessor identity

~~wherein the digital identity data is bound to the microprocessor identity using software within the digital identity device.~~

31. (Cancelled)

32. (Currently Amended) A method of identifying a property, comprising:

binding digital identity data that uniquely identifies the property to a microprocessor identity of a microprocessor operatively connected to the property, and

verifying the identity of the property by querying the microprocessor,

wherein the digital identity data is bound to the microprocessor identity,

wherein the microprocessor identity is stored in the microprocessor, and

wherein the digital identity data is bound to the microprocessor identity by encrypting the digital identity data using an algorithm that uses the microprocessor identity.

~~wherein the digital identity data is bound to the microprocessor identity using software within the digital identity device.~~

33. (Cancelled)

34. (Currently Amended) A method of securing an electronic document, comprising:
obtaining digital identity data from a digital identity device operatively connected to a computer in which the electronic document is stored;
encrypting the electronic document using the digital identity data, wherein the digital identity device comprises:
a microprocessor comprising a microprocessor identity that uniquely identifies the microprocessor, wherein the microprocessor identity is stored in the microprocessor;
a memory configured to store at least the digital identity data,
wherein the digital identity data is bound to the microprocessor identity by encrypting the digital identity data using an algorithm that uses the microprocessor identity
wherein the digital identity data is bound to the microprocessor identity using software within the digital identity device.

35. – 53. (Cancelled)

54. (Previously Presented) The method of claim 30, wherein the digital identity data comprises at least one selected from the group consisting of a name, a digital picture, an address, a date of birth, a social security number, a driver's license number, a digital photograph, biometric information, credit card information, bank account information, an incorporation name, a date and place of incorporation, a name of a corporate officer, a corporate partner, and a database administrator name.

55. – 58. (Cancelled)

59. (Previously Presented) The method of claim 32, wherein the digital identity data comprises at least one selected from the group consisting of a name, a digital picture, an address, a date of birth, a social security number, a driver's license number, a digital photograph, biometric information, credit card information, bank account information, an incorporation name, a date and place of incorporation, a name of a corporate officer, a corporate partner, and a database administrator name.

60. – 63. (Cancelled)

64. (Previously Presented) The method of claim 34, wherein the digital identity data comprises at least one selected from the group consisting of a name, a digital picture, an address, a date of birth, a social security number, a driver's license number, a digital photograph, biometric information, credit card information, bank account information, an incorporation name, a date and place of incorporation, a name of a corporate officer, a corporate partner, and a database administrator name.

65. – 68. (Cancelled)